Countrywide

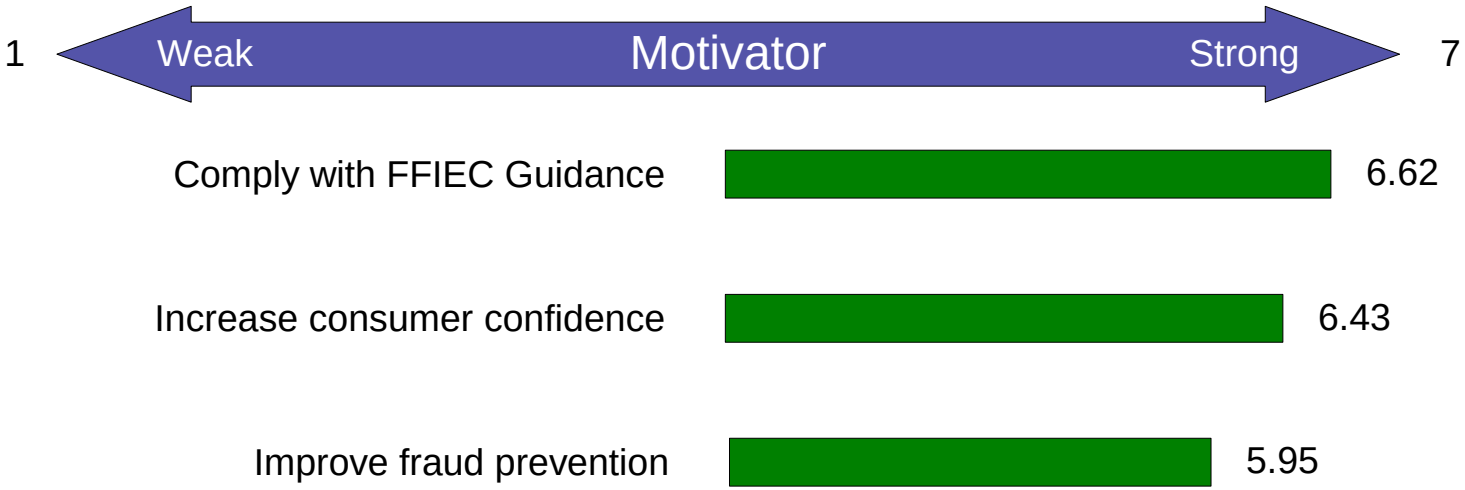
California Identity Theft Summit: Protecting Privacy Online

April 11, 2007

Christine Frye
Executive Vice President and Chief Privacy Officer
Countrywide Financial Corporation

Online Banking Security Drivers

- Motivators for implementing additional online banking security measures:



Gartner survey of 50 U.S. banks in October and November 2006

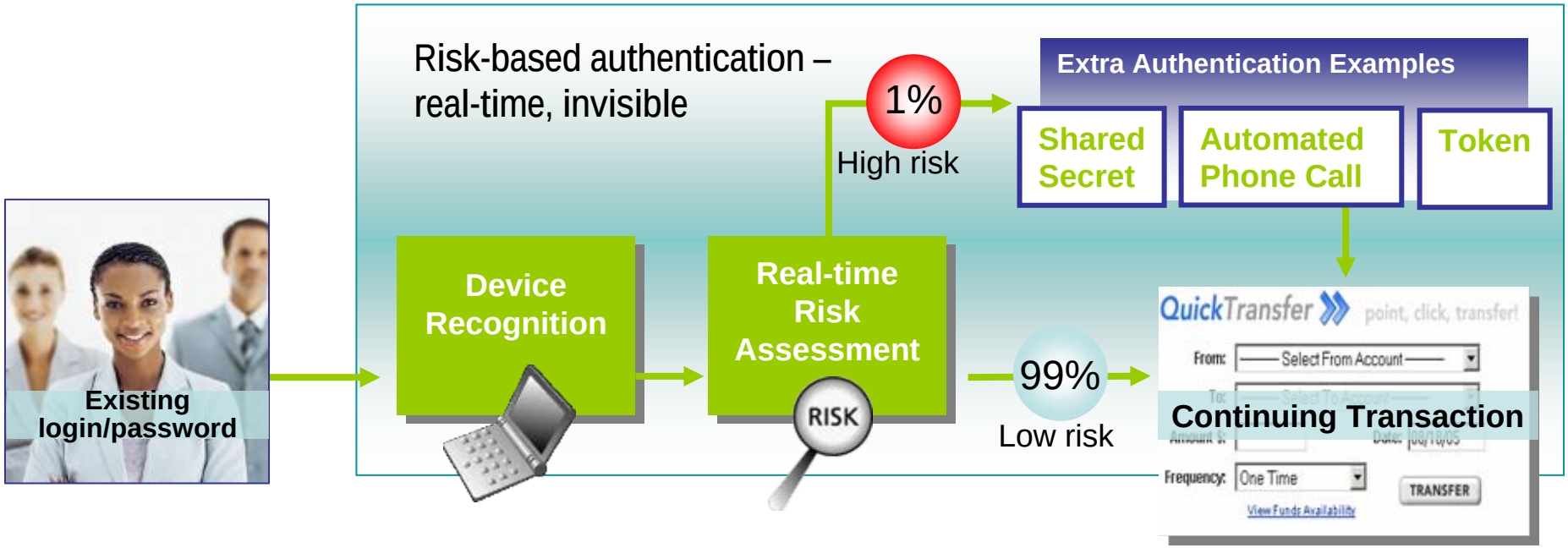
Regulatory Guidance on Online Authentication

- On October 12, 2005 the Federal Financial Institutions Examination Council (FFIEC) issued updated guidance, "Authentication in an Internet Banking Environment."
  - Focuses on protecting high risk banking processes from fraud or identify theft
  - Principles apply to all forms of electronic banking, including telephone banking systems.
  - Compliance date December 31, 2006
- Key Points:
  - Single-factor authentication, as the only control mechanism, is inadequate for high-risk transactions
  - Guidance focuses on:
    - Risk Assessments
    - Account Origination and Customer Verification
    - Monitoring and Reporting
    - Customer Awareness

Solution Considerations

- Authentication Strength vs. Total Cost of Ownership
- User Convenience
- Phishing/Sniffing Protection
- Can the technology take the financial institution into the future?
- Is the technology reusable?

Risk Based Authentication



Strong Mutual Authentication

- Provides a mutual “handshake between the customer and financial institution
  - Provides customer with a visual confirmation that they are on a legitimate site
  - Provides financial institution with additional mechanisms to validate user’s identity using IP footprinting and other challenge/response questions
- Benefits
  - Increased security beyond passwords
  - Increased confidence among online banking customers

What's a Bank Gonna Do?

- 87% of surveyed consumers said it was very important that Web sites such as online banks or stores positively and proactively identify themselves to their users.
- Banks should implement visible, convenient-to-use application that promotes consumer confidence and transparent fraud detection combined with transaction verification that detects and prevents fraudulent transactions before they are executed.
- Financial institutions that invest in additional controls beyond stronger authentication, such as fraud detection and transaction verification, will see fraud reduction that exceeds the cost of those controls by at least 25% (Gartner).

Defense In Depth

Implement complementary technologies, including fraud detection and stronger authentication and transaction verification methods to protect customer identities against all types of attacks ranging from account takeover, phishing, "pharming" and simple spyware attacks to more-sophisticated MITM and Trojan (MITB) attacks.